Exhibit 300: Capital Asset Summary

Part I: Summary Information And Justification (All Capital Assets)

Section A: Overview & Summary Information

Date Investment First Submitted: 2009-06-30
Date of Last Change to Activities: 2012-04-26
Investment Auto Submission Date: 2012-02-29
Date of Last Investment Detail Update: 2012-02-29
Date of Last Exhibit 300A Update: 2012-04-26
Date of Last Revision: 2012-04-26

Agency: 024 - Department of Homeland Security **Bureau:** 65 - National Protection and Programs Directorate

Investment Part Code: 01

Investment Category: 00 - Agency Investments

1. Name of this Investment: NPPD - National Cybersecurity Protection System (NCPS)

2. Unique Investment Identifier (UII): 024-000009508

Section B: Investment Detail

1. **Provide a brief summary of the investment, including a brief description of the related benefit to the mission delivery and management support areas, and the primary beneficiary(ies) of the investment. Include an explanation of any dependencies between this investment and other investments.**

The NCPS, operationally known as EINSTEIN, is an integrated system of intrusion detection, analytics, intrusion prevention, and information sharing capabilities that are used to defend the Federal Executive Branch civilian government?s IT infrastructure from cyber threats. The NCPS consists of the hardware, software, supporting processes, training, and services that are being developed and acquired to support the Departments mission requirements as delineated in the CNCI and mandated in NSPD-54/ HSPD-23. NSD is responsible for the development, acquisition, deployment and support required to implement the NCPS. NSD supports the Departments mission through QHSR Goal 4.1, Create a Safe, Secure, and Resilient Cyber Environment. NCPS is independent of other Department cybersecurity systems. The primary beneficiary of NCPS is the Federal Executive Branch civilian government. NCPS currently consists of discrete increments, also referred to as Blocks or EINSTEIN 2 and 3. These blocks roll out in successive but overlapping phases. EINSTEIN 2 (Block 2.0) enables the analysis of network flow information to identify potential malicious activity of traffic entering or exiting Federal Government civilian networks using signature-based intrusion detection technology. Blk 2.0 is in steady state. Block 2.1 is a spiral release of Block 2.0, and adds a Security Incident and Event Management (SIEM) solution. With the addition of this SIEM capability, the NCPS will maintain the following capabilities:

correlation of disparate data source events, data normalization, automatic correlation analysis, intelligent event monitoring, advanced threat visualization, and analytics. Blk 2.1 is in DME. Block 2.2 augments the visualization of Department and Agency threat information and provides an advanced mechanism for information sharing and collaboration, tiered to support multiple user communities. It provides a Common Operating Picture of the threat landscape of Federal Executive Branch civilian networks as generated from D/A data sets, allowing for advanced visualization, analysis, and workflow capabilities. Blk 2.2 is in DME in FY13. EINSTEIN 3 (Block 3.0) represents the next evolution of protection for civilian departments/agencies within the Federal Government. This approach will draw on commercial technology and specialized government technology to conduct intrusion prevention and threat-based decision-making on network traffic entering or leaving. Blk 3.0 is in DME.

2. **How does this investment close in part or in whole any identified performance gap in support of the mission delivery and management support areas? Include an assessment of the program impact if this investment isn't fully funded.**

The NCPS Program aligns to Quadrennial Homeland Security Review (QHSR) Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment. Specifically, the NCPS maps to and supports the objective to "Manage risks to cyberspace: Protect and make resilient information systems, networks, and personal and sensitive data." The investment addresses identified performance gaps by applying funding level scenarios to the Program's technical baseline and lifecycle cost estimate and determines achievable fiscal year performance levels depending on the funding scenario. The performance impact under the Program of Record level allows the Program to fully fund the maintenance of existing detection and analytics capabilities (Block 2.0 and 2.1), develop and deploy information sharing capabilities (Block 2.2), and develop the capacity to cover 100% of the Federal Network under Block 3.0 capabilities. However, without additional funding in FY13-17, the Program will not be able to develop the NCPS Block 2.2 information sharing capability, and will not be able to achieve Block 3.0 full operating capability (FOC) in breach of its Acquisition Program Baseline (signed by USM May 6, 2011) and agreed to in the ADE 2B decision of March 30, 2011. Without additional funding, these capabilities will not meet required performance levels.

3. **Provide a list of this investment's accomplishments in the prior year (PY), including projects or useful components/project segments completed, new functionality added, or operational efficiency achieved.**

- EINSTEIN 2 (Blk 2.) capabilities installed at 16 and operational at 15 of targeted 19 Federal D/A Trusted Internet Connection Access Providers and at all 4 Managed Trusted Internet Protocol Service vendors servicing 116 Federal Departments and Agencies. 19 MTIPS Federal D/As customers receiving EINSTEIN 2 capabilities - Completed operational testing of the Blk 2.1 SIEM analytical capability to support US-CERT in identifying patterns of malicious activity - Completed design efforts with NCPS Federal and industry partners in preparation for EINSTEIN 3 (Blk 3.0) deployments - Initiated development of EINSTEIN 3 capabilities, including 5 initial EINSTEIN 3 intrusion prevention sensors, in partnership with the NSA - Initiated development of 5 traffic aggregation points (Nests) at Internet Service Provider locations - Began work on an expanded operations environment to meet system growth, cyber watch needs, and provide alternate operational locations for US-CERT and NCCIC staff.

4. **Provide a list of planned accomplishments for current year (CY) and budget year (BY).**

FY12: - Achieve Final Operating Capability of EINSTEIN 2 by completing deployments to TICAPs for all 19 targeted Federal Departments and Agencies - Provide EINSTEIN 2 operational services to 45 Federal Department / Agency MTIPS customers - Maintain EINSTEIN 2 operational capabilities at operational TICAP and MTIPS provider locations at 99.5% system availability - Complete deployment of a Blk 2.1 SIEM analytical capability and increase data feeds to provide a more complete view of network activity - Complete operational testing and deployment of 5 EINSTEIN 3 intrusion prevention sensors at 5 Nest traffic aggregation locations, reaching Block 3.0 IOC and achieving capacity to monitor 26% of Federal Agency traffic - Procure and develop one additional EINSTEIN 3 intrusion prevention sensor and one additional Nest traffic aggregation location - Complete deployments of communications infrastructure and expanded operational environment required to operate EINSTEIN 3 capabilities FY13: - Fully maintain previously deployed Block 2.0 (detection) and Block 2.1 (analytics) capabilities - Fully maintain previously deployed EINSTEIN 3 sensors and nests.

5. **Provide the date of the Charter establishing the required Integrated Program Team (IPT) for this investment. An IPT must always include, but is not limited to: a qualified fully-dedicated IT program manager, a contract specialist, an information technology specialist, a security specialist and a business process owner before OMB will approve this program investment budget. IT Program Manager, Business Process Owner and Contract Specialist must be Government Employees.**

2009-02-27

Section C: Summary of Funding (Budget Authority for Capital Assets)

1.

Table I.C.1 Summary of Funding

	PY-1 & Prior	PY 2011	CY 2012	BY 2013
Planning Costs:	$89.4	$14.2	$18.1	$17.2
DME (Excluding Planning) Costs:	$128.0	$89.4	$106.8	$100.9
DME (Including Planning) Govt. FTEs:	$2.1	$0.0	$3.0	$3.2
Sub-Total DME (Including Govt. FTE):	$219.5	$103.6	$127.9	$121.3
O & M Costs:	$122.4	$69.2	$94.3	$216.2
O & M Govt. FTEs:	$2.5	$3.2	$5.7	$6.7
Sub-Total O & M Costs (Including Govt. FTE):	$124.9	$72.4	$100.0	$222.9
Total Cost (Including Govt. FTE):	$344.4	$176.0	$227.9	$344.2
Total Govt. FTE costs:	$4.6	$3.2	$8.7	$9.9
# of FTE rep by costs:	32	22	22	72
Total change from prior year final President's Budget ($)		$0.0	$-5.7	
Total change from prior year final President's Budget (%)		0.00%	-2.00%	

2. If the funding levels have changed from the FY 2012 President's Budget request for PY or CY, briefly explain those changes:

PY (FY11) funding levels increased to $176,016,000 from the President’s Budget request of $172,925,000 as a result of the FY11 full year CR. The CY (FY12) funding decreased to $229,000,000 due to the FY12 Omnibus Appropriations act from the FY12 President’s Budget Request of $230,602,000.

Section D: Acquisition/Contract Strategy (All Capital Assets)

Table I.D.1 Contracts and Acquisition Strategy

Contract Type	EVM Required	Contracting Agency ID	Procurement Instrument Identifier (PIID)	Indefinite Delivery Vehicle (IDV) Reference ID	IDV Agency ID	Solicitation ID	Ultimate Contract Value ($M)	Type	PBSA ?	Effective Date	Actual or Expected End Date
Awarded	7001	HSHQDC09J00490	GS23F9806H	4730							
Awarded	7001	HSHQDC11J00230	HSHQDC09D00059	7001							
Awarded	7001	HSHQDC11J00203	HSHQDC09A00032	7001							
Awarded	7001	HSHQDC11J00197	HSHQDC07D00020	7001							
Awarded	7001	HSHQDC11J00265	W91QUZ09A0003	9700							
Awarded	7001	HSHQDC11J00189	HSHQDC07D00028	7001							
Awarded	7001	HSHQDC11J00190	HSHQDC10A00102	7001							
Awarded	7001	HSHQDC11J00236	HSHQDC07D00028	7001							
Awarded	7001	HSHQDC11J00368	HSHQDC07D00020	7001							
Awarded	7001	HSHQDC11J00250	HSHQDC07D00029	7001							
Awarded	7001	HSHQDC07J00515	HSHQDC06D00032	7001							
Awarded	7001	HSHQDC10J00298	HSHQDC09D00001	7001							

2. If earned value is not required or will not be a contract requirement for any of the contracts or task orders above, explain why:
For the largest contractor support contract at NCSD with a full value of $20+ million, EVM is a contract requirement and monthly EVM and Contract Performance Reports (CPRs) are delivered. NCSD is currently conducting modifications to NCPS's prime contracts to transition them to a performance-based solution. During this transitional period, NCPS is incorporating performance-based measures into its current

contracts to approximate an earned-value solution. For example, NCPS has developed a detailed set of deliverables for its contractors as reflected in the Tailoring Plan, and has mapped these deliverables to time, schedule, budget, and work breakdown structure (WBS). This solution will provide NCPS with a mechanism to track earned value and detailed performance measures within the scope of its current contract strategy until it can fully modify its existing contracts. Monthly Program Management Reviews (PMRs) are conducted with NCPS Leadership and each contractor to review cost, schedule, scope and deliverables. In addition, time and materials contracts cannot be performance based or have earned value. All contracts that fall within FAR 34.2 include EVM and contracts that are outside of FAR 34.2 are not required to include EVM, and in most cases contain other FAR requirements that inhibit EVM.

Exhibit 300B: Performance Measurement Report

Section A: General Information

Date of Last Change to Activities: 2012-04-26

Section B: Project Execution Data

Table II.B.1 Projects

Project ID	Project Name	Project Description	Project Start Date	Project Completion Date	Project Lifecycle Cost ($M)
1	NCPS Block 2.0	NCPS Intrusion Detection Capability.			
2	NCPS Block 2.1	NCPS Analytics - Systems Information and Event Management Capability.			
3	NCPS Block 2.2	NCPS Information Sharing and Collaboration Capability.			
4	NCPS Block 3.0	NCPS Intrusion Prevention Capability.			
5	NCPS Maintenance	NCPS hardware/software system upgrades and maintenance agreements, standard technical refresh, and security patch implementation.			

Activity Summary

Roll-up of Information Provided in Lowest Level Child Activities

Project ID	Name	Total Cost of Project Activities ($M)	End Point Schedule Variance (in days)	End Point Schedule Variance (%)	Cost Variance ($M)	Cost Variance (%)	Total Planned Cost ($M)	Count of Activities
1	NCPS Block 2.0							

Activity Summary

Roll-up of Information Provided in Lowest Level Child Activities

Project ID	Name	Total Cost of Project Activities ($M)	End Point Schedule Variance (in days)	End Point Schedule Variance (%)	Cost Variance ($M)	Cost Variance (%)	Total Planned Cost ($M)	Count of Activities
2	NCPS Block 2.1							
3	NCPS Block 2.2							
4	NCPS Block 3.0							
5	NCPS Maintenance							

Key Deliverables

Project Name	Activity Name	Description	Planned Completion Date	Projected Completion Date	Actual Completion Date	Duration (in days)	Schedule Variance (in days)	Schedule Variance (%)
2	Blk 2.1 Integration & Test	Integration & Testing to implement System Analytics Capabilities; a Systems Information and Event Management Capability	2011-11-30	2012-04-30		152	-176	-115.79%
2	Blk 2.1 Implementation & Training	Implementation and Training for System Analytics Capabilities; finalize the Systems Information and Event Management Capability	2011-11-30	2011-11-30	2011-11-30	152	0	0.00%
1	Blk 2.0 Phase 2, Deployment 5 (Carryover)	Remaining Deployments to Federal Department/Agency Trusted Internet Connection Access Providers of the Intrusion Detection (EINSTEIN 2) Capability	2011-12-31	2012-06-30		183	-182	-99.45%
4	Blk 3.0 Development B	Development to implement System Intrusion Prevention (EINSTEIN 3)	2012-05-31	2012-05-31		151	0	0.00%

Key Deliverables								
Project Name	Activity Name	Description	Planned Completion Date	Projected Completion Date	Actual Completion Date	Duration (in days)	Schedule Variance (in days)	Schedule Variance (%)
		Capabilities						
4	Blk 3.0 Deployment B	Deployment for System Intrusion Prevention (EINSTEIN 3) Capabilities	2012-06-30	2012-06-30		181	0	0.00%

Section C: Operational Data

Table II.C.1 Performance Metrics

Metric Description	Unit of Measure	FEA Performance Measurement Category Mapping	Measurement Condition	Baseline	Target for PY	Actual for PY	Target for CY	Reporting Frequency
Percent of Federal Executive Branch civilian networks monitored for cyber intrusions with advanced technology	Percent	Mission and Business Results - Services for Citizens	Over target	12.900000	28.000000	29.300000	55.000000	Quarterly
Percent of unique high priority alert-level events detected by the National Cybersecurity Protection System (NCPS), validated as legitimate incidents	Percent	Customer Results - Service Quality	Over target	87.000000	90.000000	95.510000	93.000000	Quarterly
Average time in hours from automated threat identification at the threat collector to ticket generation in the incident handling system	Minutes	Process and Activities - Cycle Time and Timeliness	Under target	0.000000	15.000000	14.370000	90.000000	Quarterly
Percent of identified high vulnerabilities where mitigation strategies were provided	Percent	Technology - Effectiveness	Over target	0.000000	85.000000	90.000000	90.000000	Monthly
Average System Availability of the National Cybersecurity Protection System (NCPS)	Percent	Technology - Reliability and Availability	Over target	0.000000	0.000000		99.500000	Quarterly